DEPARTMENT OF WORKFORCE DEVELOPMENT
DIVISION OF ECONOMIC SUPPORT
ADMINISTRATOR'S MEMO SERIES

NOTICE: 99-07

ISSUE DATE: 4/28/99
DISPOSAL DATE: Ongoing

RE CARES/KIDS AND CONSUMER CREDIT REPORT SECURITY PROTECTION AND PENALTY PROCEDURES

To: Child Support Agency Directors
County Departments of Human Services Directors
County Departments of Social Services Directors
County Economic Support Managers/Supervisors
Tribal Chairpersons/Human Services Facilitators
Tribal Economic Support Directors
W-2 Agency Directors

From: J. Jean Rogers /s/
Administrator

The Division of Economic Support (DES) operates a number of programs involving confidential client information. As a matter of public trust, it is the Division's responsibility to ensure that reasonable steps are taken to safeguard sensitive and confidential client and administrative information. The securing of information involves a number of stakeholders: DES security officers, program staff, match coordinators, finance staff, facilities staff, Information Technology (IT) staff and other state and local staff. Individuals impacted by failure to safeguard sensitive information include agencies, applicants, participants and the general public.

Security can be divided into three areas: 1) systems access; 2) physical access; and 3) use of access.

- **Systems access** is access to a local area network (LAN) or mainframe. This requires logon/user IDs are password protected and fall under the province of Division IT security offices and Department IT security officers. The security officers control who has access to which systems, screens and data.

- **Physical access** means the ability to log on to a computer, to view computer screens, or obtain paper reports located in an office. This is the responsibility of the unit supervisor and facility staff. They determine if access to the work area is open or limited, and who may have pass cards and keys to access the area outside of normal hours. They can also limit access by providing locked storage cabinets or special rooms.

- **Use of access** means how those individuals with systems or physical access to confidential or sensitive information handle this access within state and federal law. This is the responsibility of agency management, the local security officer, the unit supervisor and the facility staff with access. They determine if individuals with access are using this access properly.

STEPS TAKEN TO PROVIDE ESSENTIAL ACCESS

When a new staff member is hired who requires systems access for his/her job, the **Computer Access Request** form (DES-10) and **Computer Access Request Supplement** form (DES-11) should be completed as soon as possible. If possible, local managers should complete the DES-10 and DES-11 prior to the employees' actual start date and forward the request to local security personnel. It is the duty of agency security staff (County/Tribal Security Officer, W-2 Security Officer, Functional Agency Security Liaison [FASL] or Backup Security staff) to request appropriate access for agency staff and monitor activity in the local agency to ensure state statutes are not violated. If the individual does not begin the job for some reason, contact DES security to have the logon/user ID inactivated. If logons are needed quickly, the DES-10 and DES-11 can be faxed to DES Security (608/267-0484) and the logon/user ID issued in a minimal amount of time. This eliminates the need for new staff to wait to receive access to the system. **There is no valid reason for sharing logon/user IDs.**

A logon/user ID is a unique alpha numeric identification issued to each individual who requests systems query or update access, via a DES-10 and DES-11, as approved by agency security personnel. Each request for access is specific to the individual, based on the individual's job duties, and that access must be approved by a supervisor and agency security personnel before it is sent to DES Security for entry into the security system. Each staff person using the system is granted the approved access whenever they sign into the system. Sharing of a logon/user ID by another person may give that person unauthorized access to information or transactions. If a staff person does not have the necessary system access rights, changes to the individual's access can be requested and may be granted.

If a staff member with access to any of these confidential systems leaves the agency, changes positions, or has job duties changed, the agency must request a change in access accordingly. If the employee is leaving the agency or moving to a position that there is no need for access to confidential information, the agency is responsible for immediately requesting a cancellation of all access. If the individual changes positions or job duties that requires only some of the pre-existing access, the agency must request a change in access according to the new job duties.

Wisconsin Stats., 49.124, 49.141, 49.161; 49.19; 49.22; 49.45; 49.665; 49.77 and the Department of Workforce Development (DWD) policies strictly prohibit the signing on to the computer system for use by another person, or giving an individual's logon/user ID and

password to another staff person. Local agency supervisory and management staff must not direct a staff member to either give another individual his/her logon/user ID, or to sign on to a terminal for someone else to use. This places the staff members in jeopardy of violation of DWD policy and state statutes.

TRAINING OF STAFF

All local staff must be informed of the Department's Systems Policy and State Statutes that cover computer data security. DES will hold individuals (both supervisors and staff) who violate state statutes and/or DWD Systems policy accountable. Data contained in the CARES/KIDS computer systems is confidential and must not be available to those who have not been specifically granted access to that information. For example, some staff persons have access to birth records, Social Security, or Unemployment Insurance information. DES has data sharing agreements in place with these agencies to safeguard that information. Only specific staff persons are allowed computer access to this information. In addition, any computer printouts of information, case record information, etc., must not be left where it can be accessed by others. This information must be secured in locked files.

ACCESS TO CONSUMER CREDIT REPORTS

In addition to the access listed above, some staff also have access to Consumer Credit Reports (Credit Bureaus) for purposes of locating absent parents (Child Support Enforcement), and asset identification for eligibility and benefit level determination (Economic Support). It is essential this access be used for no other purpose.

It is important agencies and workers with access to credit reports understand the nature of the system they are querying and the reasons they were granted access. When a worker enters a query to the system, several things happen. First, the worker receives personal data, such as an address, as well as credit and asset information about the individual whose record is queried. Second, the individual's Consumer Credit record is updated to record the query request. Future queries to that individual's credit record, by commercial as well as governmental entities, will show that there was a Child Support or Economic Support inquiry, which may have a negative impact on credit approval. Third, the Consumer Credit Bureau records information about the worker making the query. This worker information is provided to DES along with the monthly billing for access.

Since Consumer Credit reports are available on members of the general public, as well as our particular customer groups, it is essential that all agencies pay particular attention to the proper use of these reports. Misuse creates real harm, hence the reason for the audit trail.

Agencies should be aware that the Fair Credit Reporting Act specifically prohibits use of access to credit reports for any purpose other than authorized by law. There are penalties that will accrue to any worker using these records outside the strict business requirements of the agency. To assure the proper use of Consumer Credit Reports, workers are now required to make a case note in KIDS or CARES when they access an individual's record, indicating the reason for the query and the results.

HOW TO PROTECT SECURITY

Staff must not sign on a computer terminal and leave the machine unattended. Personal computers (PCs) must have a password protected screen saver that can be invoked when the PC is left unattended. If no password protected screen saver is available, then staff must sign off. Agencies should be aware that other non-mainframe data is not secure and must obtain appropriate screen savers in order to protect that data.

Failure to protect devices, secure passwords or safeguard material, which is confidential, means the opportunity exists for other agency staff or visitors to access data by using someone else’s logon/user ID. Once access is available to individuals who have not specifically been approved for that access, confidential information can be distributed to any number of unauthorized persons. Staff and their agency are at risk of violating Wisconsin statutes in such situations.

Confidential or sensitive information must not be left in a place for individuals who should not have access to it. Staff must use the information only when needed for job-related purposes. Information must not be used for any personal use. Both the owner of the logon/user ID and the individual accessing the computer system with another person's logon/users ID can be held accountable for the violation of state statute.

Systems audit trails have been developed which identify individuals, records accessed, screens accessed, what the worker was doing (adding, creating, updating or deleting data), the computer terminal ID used and the day and time it took place. Any activity taking place using this logon/user ID is the responsibility of the individual to whom it was issued.

Violations of the policy or state statutes will be investigated as follows:

- **First offense:** Logon will be suspended until the agency security officer/supervisor calls DES Security and verifies the offense has been discussed.

- **Second offense:** Logon will be suspended for three-work days and then will be released for use when the agency security officer/supervisor calls DES Security and verifies the offense has been discussed.

- **Third offense:** Logon will be deleted and future access denied.

Multiple offenses, from the same agency, may result in suspension of access for the entire agency or other corrective action may be required.

(NOTE: These penalties may be increased, if required by federal law or policy. In particular, federal law provides for civil and criminal penalties for failure to limit access to consumer credit reports and social security records to the specific purposes outlined in law.)

DES Security will monitor the use of logon/user IDs and systems activity when there is a suspected security violation. If there is misuse, the logon/user ID will be suspended. County/Tribal/W-2 security officers have the responsibility to determine if the violation was intentional or unintentional. The logon/user ID will not be reinstated by the Division Security staff until the County, Tribal or W-2 security officer makes such a request. If the local security officer is not available, it is appropriate for the worker's supervisor to request the suspension be lifted. DES Security will also monitor CARES and KIDS for the required case note regarding Consumer Credit Report queries.

During the time period access is denied, staff will be unable to perform that portion of their job requiring computer access. Loss of access to the system may place a staff person in jeopardy of being unable to perform the functions of the job. Supervisors who require a staff member to allow access to another person will receive the same suspension of access.

Anyone who becomes aware of what appears to be inappropriate use of logons should immediately call the Security Call Center (608/261-6827). Security staff will assist the logon/user to identify and resolve the problem.

DES reserves the right to deny access to persons who violate systems security statutes, department procedures or administrative requirements for confidentiality as described in the *Income Maintenance Manua*l Chapter II, Part B, and *Child Support Policy and Program Manual*, Chapter 12, Part 3.7.

Here are some “good business practices” to serve as examples:

- If paper or printouts are used, items with client specific data should be secured when the user leaves the area; either at the end of the day or for a break. "Secured" means; a locked file cabinet may be used for very sensitive information (IRS data, W-2, Medicaid, Food Stamp and Child Care program eligibility data, domestic violence, etc.) or a locked desk drawer might be suitable depending on how accessible the office is to non-authorized staff or the public.

- Room keys and building access cards must be carefully tracked to verify who was in the building in case there is an accident or theft.

- Staff working evenings or weekends must lock the doors after they leave to secure the office equipment and paper information.

- Computer passwords must never be written down or posted anywhere.

- Personal Computers must have password protected screen savers.

- Sign-off from mainframe terminals when staff are not present.

- When Consumer Credit Reports are queried for an individual, staff making the query **must** make a case note in KIDS or CARES indicating the reason for the query and the result.

In summary, agencies need to ensure that reasonable and prudent procedures are in place to control access to information, geared toward protecting the privacy of individuals. However, the information needs to be readily available to those who need it to do their assigned tasks.

REGIONAL OFFICE CONTACT: DES Area Administrator

CENTRAL OFFICE CONTACT: DES Security Unit
608/261-6827